News

The EU Cyber Resilience Act: Implications for Companies

21 November 2024

The EU Cyber Resilience Act (CRA) (Regulation (EU) 2024/2847) is a pioneering piece of EU legislation that establishes mandatory cybersecurity standards for most hardware and software products made available on the EU market. The CRA enters into force on 10 December 2024 and leaves companies a period of three years to ensure that products with digital elements meet the CRA's requirements in order to remain eligible for sale in the EU. Non-compliance with the CRA can lead to administrative orders and substantial fines. This article offers an overview on the CRA and recommended steps companies can take to ensure compliance.

Chapter **1 1**

Background and Timeline

The CRA was adopted to address the growing popularity of digital products and increasing cybersecurity risks. After its publication in the EU Official Journal, the CRA will enter into force on **10 December 2024**. Its overall applicability will commence after a three year period on 11 December 2027 (Art. 71 CRA), thereby giving companies time to implement the CRA requirements. Certain provisions on the notification of conformity assessment bodies will already apply from 11 June 2026. Also, manufacturers must comply with reporting obligations with regard to actively exploited vulnerabilities and severe incidents concerning their digital products from 11 September 2026.

Chapter **2 2**

Scope of Application

Material Scope

The CRA's material scope is very broad and generally includes all "**products with digital elements**" that are made available on the EU market, and whose "intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network" (Art. 2(1) CRA). Such products with digital elements include all software or hardware products and their remote data processing solutions, including separately sold software or hardware components (Art. 3 no. 1 CRA).

The broad wording of this definition allows the CRA to cover a wide range of products, ranging from consumer products (e.g. IoT devices, B2C apps) to industrial systems. Cloud computing solutions can only be regarded as remote processing solutions to the extent they align with the criteria set forth under the CRA (see Art. 3 (2) CRA). Free and open-source software is only subject to the CRA to the extent it is intended for commercial activities (Recital (19) CRA).

In order for the CRA to be applicable, relevant products must be "**made available on the market**". This encompasses supplying a product for distribution or use within the EU market during **commercial activities**, whether for payment or free of charge (Art. 3 (22) CRA; see Recital (15) CRA for further examples of commercial activities).

While the CRA's objective is to set extensive cybersecurity standards for products with digital elements made available on the EU market, it allows for **exceptions** for specific products (Art. 2(2)-

(8) CRA): Products that are subject to specific EU regulations, spare parts, products developed or modified exclusively for national security or defence purposes and products specifically designed to process classified information.

Personal Scope

The CRA addresses various "**economic operators**" along the supply chain, including manufacturers, authorized representatives, importers and distributors (Art. 3 (12) CRA). Further, it stipulates a separate set of obligations that applies to open-source software (OSS) stewards (Art. 3 (14) CRA).

Territorial Scope

With regard to the territorial scope of the CRA, the marketplace principle applies and the regulatory framework encompasses all products with digital elements made available on the EU market (Art. 2(1), 3 (22) CRA). In consequence, the CRA has implications for economic operators within and outside the EU, if they make products with digital elements available on the EU market or seek to significantly modify products already made available on the EU market once the CRA is in effect.

Chapter **3 3**

Classification of Products

The set of CRA obligations applicable to a product with digital elements depends on the cybersecurity risk level associated with the product category. In particular, the CRA differentiates between critical, important (class I and II), and non-critical products, whereby the latter are estimated to account for 90% of products on the EU market.

Product category	**Description and Relevant Provisions**	**Examples (non-exhaustiv**
Non-critical ~ 90% of products	General requirements (Art. 6 CRA)	Photo editing software, tex processing software, hard drives, games, smart home products without security functions

Important (class I)	Core functionality of one of the product categories listed in Annex III CRA 1.Either primarily performs functions that are critical to the cybersecurity of other products, networks or services, or 2.performs a function that carries a significant risk of adverse effects with regard to its intensity and ability to disrupt, control or cause damage to (i) a large number of products, or (ii) the health, security or safety of its users through direct manipulation (Art. 7(2) CRA) General + additional requirements (Art. 6 and 7 CRA)	Identity management syste and hardware, browsers, password managers, netwo management systems, operating systems, routers modems, public key infrastructure, smart home products with security func (Annex III CRA)
Important (class II)	Core functionality of one of the product categories listed in Annex III CRA Same criteria as class I (Art. 7(2) CRA) General + additional requirements (Art. 6 and 7 CRA)	Container or virtual machir firewalls, intrusion detectio and prevention systems, tamper-resistant microprocessors and microcontrollers (Annex III
Critical	Core functionality of one of the product categories listed in Annex IV CRA 1.Either critical dependency of essential entities pursuant to Art. 3 NIS2 Directive on the product category, or 2.the potential of serious disruptions to critical supply chains across the EU market as a result of incidents and exploited vulnerabilities concerning the product category (Art. 8(2) CRA, Recital (46) CRA). General + additional requirements (Art. 6 and 8 CRA)	Hardware devices with sec boxes, smart meter gatewa within smart metering syste and other devices for adva security purposes, includin secure cryptoprocessing, smartcards or similar devic including secure elements (Annex IV CRA)

Chapter **4 4**

Key Obligations

The CRA establishes a comprehensive framework of cybersecurity obligations on economic operators involved in the supply chain of products with digital elements, even imposing a distinct set of obligations on OSS stewards.

- Due to the crucial role of **manufacturers** in the design and production of hardware and software, the CRA imposes a broad set of obligations on them that cover the entire product lifecycle (Art. 13, 14 CRA), including obligations to
  - establish the required **essential cybersecurity standards** already at the beginning of the product lifecycle (i.e. product development stage);
  - prior to introducing the product on the EU market, perform a **conformity assessment** to verify that the

requirements set out by the CRA are met;

- create required **documentation**, including **technical documentation** as well as **information and instructions for users**;

- after market release, comply with the relevant regulations concerning the **monitoring** of product compliance and update of relevant documentation, as well as obligations regarding the ongoing **vulnerability management** and the associated **notification** obligations.

- **Importers** play an essential role regarding the introduction of products on the EU market produced by third country manufacturers. They are required to ensure that products with digital elements placed on the EU market comply with the essential cybersecurity requirements and vulnerability handling processes under the CRA. Importers are also obliged to verify that other key requirements for manufacturers under the CRA have been fulfilled, such as the performance of an appropriate conformity assessment by the manufacturer or the existence of adequate technical documentation.

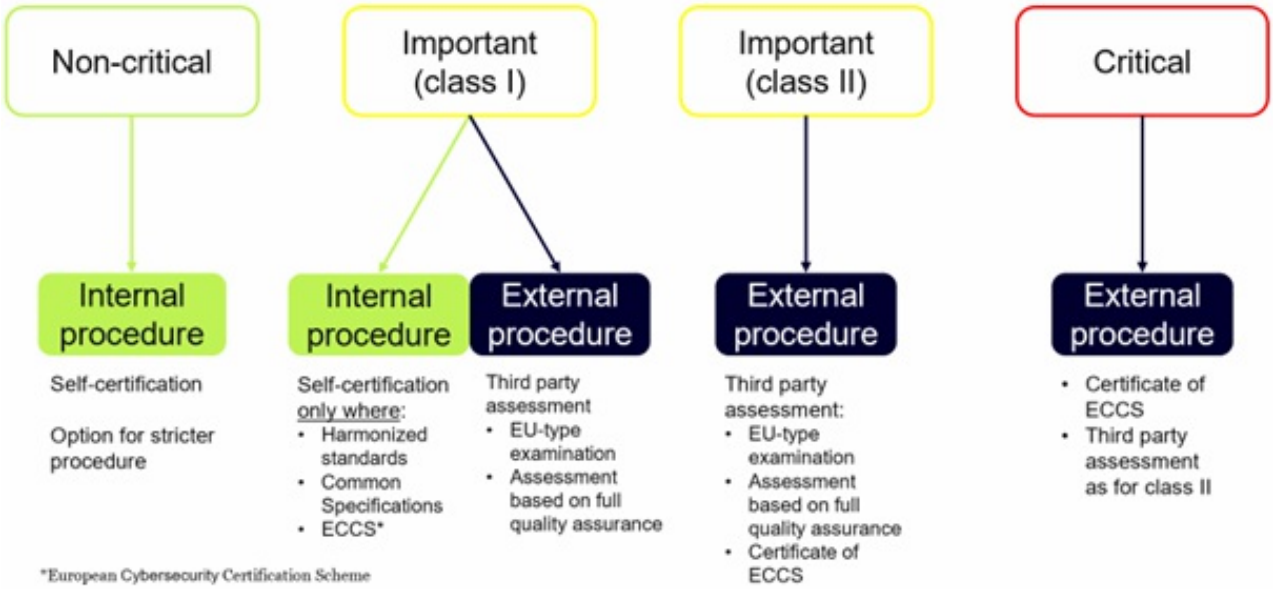
- **Distributors** must verify that the product with digital elements bears the CE marking before making it available on the EU market, (Art. 20(2)(a) CRA), as well as that key requirements for manufacturers and importers under the CRA have been fulfilled (Art. 20(2)(b) CRA).

- The obligations for **OSS stewards** were incorporated during the final negotiation phase for the CRA, in response to significant concerns that the CRA will also apply to the open-source industry. In consequence, looser standards were established (Art. 24 CRA, Recital 19 CRA).

Chapter **5 5**

Conformity Assessment Procedures

A crucial part of the obligations of the manufacturer set out by the CRA is the performance of the conformity assessment (Art. 13(12), 32 CRA). This is the process of verifying whether the essential cybersecurity requirements set out in Annex I have been fulfilled (Art. 3 (27) CRA). First, it is necessary for manufacturers to identify products with digital elements and then classify these products in the beforementioned product categories, as different procedures apply to the distinct product classes. The CRA mainly distinguishes between internal and external procedures.



After successfully performing the relevant conformity assessment procedure, the manufacturer is obliged to draw up the **EU declaration of conformity** (Art. 28 CRA) and affix the Conformité Européenne CE-marking (Art. 29, 30 CRA).

Chapter **6 6**

Steps for Compliance

It is likely that the majority of companies involved in the production and distribution of hardware or software products on the EU market will be affected by the CRA in some way. Therefore, it is advisable to take the necessary steps to ensure compliance with the CRA.

Even though most of the obligations imposed by the CRA **will not come into full effect until 11 December 2027**, it is still recommended that companies commence CRA compliance projects as soon as possible. This applies in particular in light of product development and release timelines, given that the requirements of the CRA will impact these stages of the product lifecycle significantly.

In order to ensure CRA compliance, companies could take the following practical steps:

1. **Applicability assessment**: Determine against a product inventory the relevant software, hardware and remote processing products with digital elements and the respective role as economic operator under the CRA.

2. **Classification of products**: Determine for each product in the inventory whether it falls into the non-critical, important, or critical category

3. **Gap analysis**: Perform an assessment the applicable CRA obligations to identify any existing compliance gaps for the relevant products.

4. **Action item specification**: Use the gap analysis and list of identified products to identify the specific action items needed for compliance with the CRA; determine and allocate resources (financial, human, technological) necessary for implementation of actions items.

5. **Implementation of compliance measures**: Create a project plan for the implementation of the measures that address the identified action items, depending on the role, where required in parallel to the product design and development process. Where possible, CRA compliance should be integrated into existing product conformity assessment procedures.

Companies should consider their individual situation to further specify the relevant steps required to comply with the CRA and should keep a close eye on the ongoing legal developments related to the CRA, including the development and adoption of harmonized standards as well as the appointment of responsible notified conformity assessment bodies.

Authored by Dr. Henrik Hanssen and Anna Theresa Vogel.

Contacts

Henrik Hanssen

Counsel

Hamburg

Email me

Anna Theresa Vogel

Associate

Berlin

Email me